PP Docket no 92-234

THOMSON CONSUMER ELECTRONICS

600 North Sherman Drive, Indianapolis IN 46201-2598 USA • Tel: (1 317) 267-5000

Date: December 21, 1992

To: Federal Communication Commission
1919 M Street
NW Washington, DC 20554

ATTENTION RAY LAFORGE/SATELLITE BRANCH

From: Bill Beyers
Thomson Consumer Electronics
600 N. Sherman Drive
Indianapolis, IN 46201

Subject: NOTICE OF INQUIRY ON ENCRYPTION STANDARDS FOR SATELLITE DELIVERED SIGNALS

We see two conflicting considerations that must be balanced in reflecting on the issue of selecting a standard for Satellite delivery of television. The major benefit of a standard is that it removes monopolistic barriers to program delivery, which may be important when an industry is in its infancy, but which in the long run do not service the public interest or that of the industry in general. The major drawback of setting a standard is that the existence of such a standard may impede the application of advanced technology to the service and thus reduce the services that might otherwise be available to the public. It is, of course, the task of the commission to weigh and consider these issues and decide which course is in the public interest.

The present environment in this industry makes this task especially difficult. The industry is in the initial phases of changing technology from its present analog delivery system to a system of delivering television by digital modulation of compressed digital video. One must give consideration to the scope of the problem and decide whether the object is to have an encryption system that works for both technologies, or a separate system for each, or a standard for only one technology.

Which every goal is selected, we believe the elements of a good solution are:

1) Hardware partitioning of video and audio "descrambling" and key decryption. Basically, the signal processing hardware should contain no secrets and should be such that it can be manufactured by any supplier interested in the business. This hardware will contain standard hardware for descrambling audio and video. However, this descrambling hardware requires a key as an input to deliver the correct descrambled output. An example of such a system is a DES descrambler. This system takes in data in 64 bit blocks and uses 56 bit keys to direct the re-arrangement of the bits to produce 64 bits of descrambled information. (An interesting advantage of block scrambling is that special resynchronization is not required if the blocks of data are lost.)

2) Use of Smartcards for key decryption. Smartcards have been especially engineered to provide physical security for the secrets that may be included in the microcomputers contained on the Smartcards. And perhaps as important, they are relatively inexpensive and can be cheaply and easily replaced if the security system is breached. This limits the potential financial loss because of the speed and ease at which systems can be changed and further deters attack because of the certain knowledge that gains of the attacker will be limited.

3) Independence of program suppliers. By this we mean that any program supplier can operate his own encryption and billing system without any secret knowledge of anyone else's system. This can be easily achieved if the program supplier supplies his own Smartcards with his own decryption algorithm. It is also possible for several suppliers to contract with one Smartcard supplier to supply a single Smartcard that will serve several systems.

4) Downloadable "verifier" and standard software interface. Since the microcomputer on the Smartcard is necessarily small to meet price objectives, it is necessary to have software in the control microcomputer of the signal processing hardware to carry out interface tasks. These include interface between incoming data for key generation which must be sent to the Smartcard, key outputs from the Smartcard that must be transferred to the appropriate descrambler in the signal processing hardware, and messages from the entitlement processor contained in the Smartcard that must be sent to the user, usually via some text display in the video. Since this software will vary with program supplier, it is probably best to reserve some RAM in the control microprocessor and allow program suppliers to download their own program for this processing. This program must be in a high level language specialized for this task, essentially a set of subroutine calls to standardized subroutines contained in ROM in the control microcomputer.

If a standard is partitioned as above, it is easy to see that the essential difference between a digital and an analog system is the "scrambling hardware", not the key decryption system. Thomson presently supplies consumer priced hardware for scrambling and decryption of satellite based analog delivery systems that include video scrambling that is far superior to that offered by present Video Cypher units. This system is Smartcard based and has the advantages mentioned above. Because of its technical inferiority and because of the monopolistic position it provides its supplier, and its lack of resistance to sustained attacks, we would strongly oppose standardization of the Video Cypher system for satellite delivery of analog television signals.

For future delivery systems based on digital compression, we believe the opportunity exists to select a Smartcard based encryption standard which partitions the hardware as mentioned above. Although we see it is possible to design a Smartcard based system which could work for both analog and digital systems, it has not been clear to us that the evolution of the industry would require such a product.